

(51)Int.Cl.  
H 04 L 12/40  
9/00  
9/10

識別記号

序内整理番号

F I

技術表示箇所

7341-5K

H 04 L 11/ 00

3 2 0

9/ 00

Z

審査請求 未請求 請求項の数 3 O L (全 9 頁) 最終頁に続く

(21)出願番号

特願平5-314617

(22)出願日

平成5年(1993)12月15日

(71)出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72)発明者 小林 秀樹

東京都大田区中馬込1丁目3番6号 株式  
会社リコー内

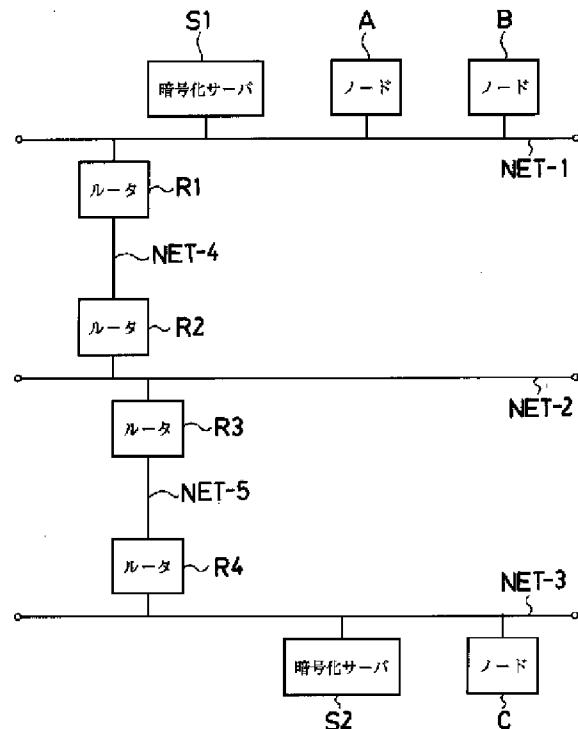
(74)代理人 弁理士 大澤 敬

(54)【発明の名称】 ローカルエリアネットワーク

(57)【要約】

【目的】 各端末装置でデータの暗号化と復号化を行なわなくとも端末装置間でデータを暗号化して送受信できるようにする。

【構成】 I PネットワークNET-1の送信元の端末装置であるノードAから送信される元データを暗号化サーバS1が暗号化データに変換してノードAへ返送し、ノードAはその暗号化されたデータをI PネットワークNET-3の送信元の端末装置であるノードCへ送る。一方、I PネットワークNET-3の受信先の端末装置であるノードCから送信される暗号化データを暗号化サーバS2が解読して元データに復元してノードCへ返送する。



## 【特許請求の範囲】

【請求項 1】 複数の端末装置間でデータを送受信可能にネットワークで接続し、該ネットワークに、送信元の端末装置から送信される元データを暗号化データに変換して該送信元の端末装置へ返送し、受信先の端末装置から送信される暗号化データを解読して元データに復元して該受信先の端末装置へ返送する手段を有する暗号化サーバを設けたことを特徴とするローカルエリアネットワーク。

【請求項 2】 複数の端末装置間でデータを送受信可能に接続したネットワークを複数接続し、該各ネットワークに、送信元の端末装置から送信される元データを暗号化データに変換して他のネットワークの受信先の端末装置へ送信し、他のネットワークから受信した暗号化データを解読して元データに復元して受信先の端末装置へ送信する手段を有する暗号化サーバを設けたことを特徴とするローカルエリアネットワーク。

【請求項 3】 請求項 1 記載のローカルエリアネットワークにおいて、

前記各端末装置が、前記暗号化サーバに対してデータの暗号化又はその解読に必要な暗号化キーを送信する手段を有し、前記暗号化サーバが、前記各端末装置から受信した暗号化キーに基づいてデータの暗号化又はその解読を行なう手段を有することを特徴とするローカルエリアネットワーク。

## 【発明の詳細な説明】

### 【0 0 0 1】

【産業上の利用分野】 この発明は、複数の端末装置をネットワークを介して接続したローカルエリアネットワークに関する。

### 【0 0 0 2】

【従来の技術】 従来、Ethernet や IEEE 802.3 等の規格のローカルエリアネットワーク（以下「LAN」と略称する）では、各端末装置（以下「ノード」と略称する）間で送受信するパケットの内容の秘密を守るために、送信側のノードで送信すべきパケットの内容を所定の暗号系によって暗号化して相手先のノードへ送信し、その相手先である受信側のノードではその受信した暗号化されたパケットを解読して元のデータ内容に復元していた。

【0 0 0 3】 この暗号系は、誰が読んでも理解できる情報を予め決められた暗号化キー（単に「キー」とも称する）に基づいて意味の分からぬ暗号文に変換し、その暗号文を暗号化されたときに使用した同じ暗号化キーに基づいて解読して元の情報を復元（これを「復号化」と称する）する技術である。

【0 0 0 4】 一般に、暗号系としては標準暗号に制定されているDES暗号法、FEAL暗号法等の共通キー暗号系が知られており、その共通キー暗号系は、送受信者間で等しい暗号化キーと復号化キーを共有し、その共通

のキーでデータの暗号化と復号（復元）化を行なう方法である。

### 【0 0 0 5】

【発明が解決しようとする課題】 しかしながら、上述した従来の LAN では、通信の秘密を守るためにパケットの暗号化が標準化（規格化）されていないため、送信側のノードでパケットの内容を暗号化して送信し、受信側のノードでその受信したパケットの暗号化されたデータ内容を解読して元のデータに復元しなければならなかつた。

【0 0 0 6】 したがって、各ノードの処理負担がかかってしまううえに、暗号化キーの変更や暗号系（暗号化方式）の変更時に、LAN 上の全てのノードの設定変更を行なわなければならなくなつて大変不便であるという問題があつた。

【0 0 0 7】 また、ローカルなネットワーク環境ではネットワークが管理状態に置かれていおり、または管理し易いので、ネットワークの信頼性は高いが、外部のネットワークを介して複数のネットワーク間の端末装置間で通信を行なえるようにした場合、データがどのようなネットワークの経路を通つて送受信されて相手に到達するのか分からないので、途中で外部のものにデータ内容を覗かれてしまう危険があるという問題も有つた。

【0 0 0 8】 この発明は上記の点に鑑みてなされたものであり、各端末装置でデータの暗号化と復号化を行なわなくとも端末装置間でデータを暗号化して送受信できるようにすることを目的とする。

### 【0 0 0 9】

【課題を解決するための手段】 この発明は上記の目的を達成するため、複数の端末装置間でデータを送受信可能にネットワークで接続し、そのネットワークに、送信元の端末装置から送信される元データを暗号化データに変換してその送信元の端末装置へ返送し、受信先の端末装置から送信される暗号化データを解読して元データに復元してその受信先の端末装置へ返送する手段を有する暗号化サーバを設けたローカルエリアネットワークを提供する。

【0 0 1 0】 また、複数の端末装置間でデータを送受信可能に接続したネットワークを複数接続し、その各ネットワークに、送信元の端末装置から送信される元データを暗号化データに変換して他のネットワークの受信先の端末装置へ送信し、他のネットワークから受信した暗号化データを解読して元データに復元して受信先の端末装置へ送信する手段を有する暗号化サーバを設けたローカルエリアネットワークも提供する。

【0 0 1 1】 さらに、上記のようなローカルエリアネットワークにおいて、上記各端末装置が、上記暗号化サーバに対してデータの暗号化又はその解読に必要な暗号化キーを送信する手段を有し、上記暗号化サーバが、上記各端末装置から受信した暗号化キーに基づいてデータの

暗号化又はその解読を行なう手段を有するようにするといふ。

#### 【0012】

【作用】この発明によるローカルエリアネットワークは、ネットワークに設けた暗号化サーバが、送信元の端末装置から送信される元データを暗号化データに変換してその送信元の端末装置へ返送し、受信先の端末装置から送信される暗号化データを解読して元データに復元してその受信先の端末装置へ返送するので、各端末装置でデータの暗号化と復号化を行なわなくても端末装置間でデータを暗号化して送受信できる。

【0013】また、それぞれ接続された複数のネットワークに設けた暗号化サーバが、送信元の端末装置から送信される元データを暗号化データに変換して他のネットワークの受信先の端末装置へ送信し、他のネットワークから受信した暗号化データを解読して元データに復元して受信先の端末装置へ送信するので、各端末装置でデータの暗号化と復号化を行なわなくても異なるネットワーク間の端末装置間でデータを暗号化して送受信できる。

【0014】さらに、各端末装置が、暗号化サーバに対してデータの暗号化又はその解読に必要な暗号化キーを送信し、暗号化サーバが、各端末装置から受信した暗号化キーに基づいてデータの暗号化又はその解読を行なうようにすれば、その暗号化キーに基づく暗号化方式によつて暗号化及び復号化を行なえる。

#### 【0015】

【実施例】以下、この発明の実施例を図面に基づいて具体的に説明する。図1は、この発明の一実施例のローカルエリアネットワーク（LAN）のシステム構成を示す図である。このローカルエリアネットワークではTCP/IPプロトコルを用いている。このローカルエリアネットワークは、3つのIPネットワークNET-1、NET-2、NET-3がある。

【0016】IPネットワークNET-1には、CPU、ROM、及びRAMからなるマイクロコンピュータを内蔵した端末装置（ノード）AとBが接続されており、同じくマイクロコンピュータを備えた端末装置の一種であつてノードAとBのデータを暗号化及びその解読（復元）をする暗号化サーバS1が接続されており、2ネットワーク間でパケットのルーティングを行なうルータ（「ゲートウェイ」とも称する）R1が接続されている。

【0017】また、IPネットワークNET-2には、2ネットワーク間でパケットのルーティングを行なうルータR2とR3が接続されている。さらに、IPネットワークNET-3には、マイクロコンピュータを内蔵したノードCが接続されており、同じくマイクロコンピュータを備えた端末装置の一種であつてノードCのデータを暗号化及びその解読（復元）をする暗号化サーバS2が接続されており、2ネットワーク間でパケットのル

ーティングを行なうルータR4が接続されている。

【0018】そして、ルータR1とR2はネットワークNET-4によって結ばれており、ルータR3とR4はネットワークNET-5によって結ばれており、IPネットワークNET-1とNET-3の各ノードA、B、C間でデータを送受信することができ、その際、暗号化サーバS1とS2によってデータを暗号化し、受信した暗号化データを復号化する（これを「暗号化通信」と称する）ことができる。

【0019】上記暗号化サーバS1とS2は、送信元の端末装置から送信される元データを暗号化データに変換してその送信元の端末装置へ返送し、受信先の端末装置から送信される暗号化データを解読して元データに復元してその受信先の端末装置へ返送する手段を有しており、この場合、暗号化及びその解読のための暗号化キーは同じであつて暗号化アルゴリズムが同じである。

【0020】図2は、IPネットワークNET-1のノードAからIPネットワークNET-3のノードCへ暗号化通信を行なうときのデータの流れを示すフローチャートである。ここでは、暗号化サーバS1とS2の暗号化キー（キーコード）は固定されている場合について説明する。

【0021】まず、初期化時、ノードAはローカルエリアネットワークの暗号化サーバS1のアドレスを登録し、ノードCはローカルエリアネットワークの暗号化サーバS2のアドレスを登録する。

【0022】ノードAは、1パケットの送信要求が発生すると、暗号化サーバS1へ「暗号化要求フラグ」を立てて生データを送信する。暗号化サーバS1は、ノードAから受信した生データを暗号化キーを用いて予め設定されている暗号化方式によって暗号化し、「暗号化済フラグ」を立ててノードAへ返送する。

【0023】そして、ノードAは暗号化サーバS1から受信した暗号化データを暗号化データを示す情報を付加してIPネットワークNET-3のノードCへ送信（転送）する。その暗号化データであることを示す情報は、暗号化データのパケットのヘッダ部に格納すると良い。

【0024】一方、ノードCは、ノードAから受信したパケットのヘッダ部を調べて、暗号化データであることを示す情報が格納されていれば、そのパケットが暗号化データであると判断し、その暗号化データに「解読要求フラグ」を立てて暗号化サーバS2へ転送する。暗号化サーバS2は、ノードCから受信した暗号化データを暗号化キーを用いて解読して復元し、「解読済フラグ」をセットしてノードCへ返送する。ノードCは、暗号化サーバS2から復元されたデータを得る。

【0025】このようにして、ネットワーク毎にデータの暗号化及びその解読を行なう暗号化サーバを設け、その暗号化サーバがネットワーク上の各端末装置に送受信されるデータの暗号化及びその解読を一括して処理する

ので、各端末装置がデータの暗号化及びその解読に係る処理を行なわずに済む。

【0026】図4はパケットのIPヘッダのフォーマットを示す図、図5はそのIPヘッダの「(オプション) Options」フィールドのフォーマットを示す図である。上記の暗号化要求フラグ、暗号化済フラグ、解読要求フラグ、及び解読済フラグはIPヘッダの「Options」

フィールドのオプションエリアに定義する。

【0027】表1はオプション・データの一例を示す表であり、上記各フラグは、例えば、暗号化要求フラグ「0」、暗号化済フラグ「1」、解読要求フラグ「3」、解読済フラグ「4」である。

【0028】

【表1】

Class	Number	長さ	機能
0	0	1	オプション・リストの終わり
0	1	1	NOP(オペレーション無し)
0	2	11	セキュリティと処理に対する制約
0	3	可変	Loose Source Routing
0	9	可変	Strict Source Routing
0	7	可変	ルート記録
0	8	4	ストリーム識別子
2	4	可変	時刻印
1	1	1	フラグ 0 暗号化要求 1 解読要求 2 暗号化済 3 解読済

【0029】次に、IPネットワークNET-1のノードAからIPネットワークNET-3のノードCへ暗号化通信を行なうとき、データの暗号化及びその解読のための暗号化キーを暗号化サーバS1とS2へ送る場合の例について説明する。

【0030】この場合、各ノードA、Cはデータの暗号化又は解読のための暗号化キーを暗号化サーバS1、S2へ送信する機能を有し、暗号化サーバS1、S2は複数の暗号化キーを用いた暗号化及びその解読方式を行なう機能をそなえており、ノードA、Cから送信される暗号化キーを用いてデータの暗号化及びその解読を行なう機能を果たす。

【0031】まず、ノードAはノードCとの間で暗号化データをやり取りするために必要な暗号化キーの共通化を図る初期化通信を行なう。この初期化通信によって、ノードAとノードCは同じ暗号化方式の暗号化キーを所持することになる。

【0032】そして、ノードAから暗号化サーバS1へ元データを送るとき、暗号化キーを貼付し、暗号化サーバS1はその暗号化キーを使用して元データを暗号化する。また、暗号化データの解読時には、ノードCは暗号化サーバS2へ解読を依頼するときその暗号化キーを添付し、暗号化サーバS2はその暗号化キーを使用して暗号化データを復元する。暗号化キーは、例えば、図4及び図5に示したIPヘッダの「オプション・データ」に定義する。

【0033】ノードAは、1パケットの送信要求が発生すると、暗号化サーバS1へ「暗号化要求フラグ」を立

てて暗号化キーと共に生データを送信する。暗号化サーバS1は、ノードAから受信した生データをその暗号化キーを用いた暗号化方式によって暗号化し、「暗号化済フラグ」を立ててノードAへ返送する。そして、ノードAは暗号化サーバS1から受信した暗号化データをIPネットワークNET-3のノードCへ送信(転送)する。

【0034】一方、ノードCはノードAから暗号化データを受信すると、その暗号化データを「解読要求フラグ」を立てて暗号化キーと共に暗号化サーバS2へ転送する。暗号化サーバS2は、ノードCから受信した暗号化データをその暗号化キーを用いた解読方式によって復元し、「解読済フラグ」をセットしてノードCへ返送する。ノードCは、暗号化サーバS2から復元されたデータを得る。したがって、このLANではキーコードを可変にすることができる。

【0035】次に、IPネットワークNET-1のノードAからノードBへ暗号化通信を行なうとき、データの暗号化及びその解読のための暗号化キーを暗号化サーバS1へ送る例について説明する。

【0036】ノードAは、1パケットの送信要求が発生すると、暗号化サーバS1へ「暗号化要求フラグ」を立てて暗号化キーと共に生データを送信する。暗号化サーバS1は、ノードAから受信した生データをその暗号化キーを用いた暗号化方式によって暗号化し、「暗号化済フラグ」を立ててノードAへ返送する。そして、ノードAは暗号化サーバS1から受信した暗号化データをノードBへ送信(転送)する。

【0037】一方、ノードBはノードAから暗号化データを受信すると、その暗号化データを「解読要求フラグ」を立てて暗号化キーと共に暗号化サーバS1へ転送する。暗号化サーバS1は、ノードBから受信した暗号化データをその暗号化キーを用いた解読方式によって復元し、「解読済フラグ」をセットしてノードBへ返送する。ノードBは、暗号化サーバS1から復元されたデータを得る。

【0038】このようにして、各端末装置が暗号化サーバにデータの暗号化及びその解読を依頼するとき、データと共にその暗号化及び解読に必要な暗号化キーを送り、暗号化サーバは、その暗号化キーに基づいた暗号化方式でデータの暗号化及びその解読を行なうので、各端末装置では多様な暗号化方式によるデータ送受信を容易に利用することができる。また、各ノードが自由に暗号化キーを設定して、データの暗号化方式を選択できるので、さらにデータ通信の機密性を高めることができる。

【0039】次に、暗号化サーバにネットワークルーティング機能を設けたときの暗号化通信の例について説明する。この場合のネットワーク構成は図1に示したローカルエリアネットワークと同じであるが、各ノードA、B、Cと暗号化サーバS1、S2の機能が若干異なる。

【0040】この例の暗号化サーバS1とS2は、送信元の端末装置から送信される元データを暗号化データに変換して他のネットワークの受信先の端末装置へ送信し、他のネットワークから受信した暗号化データを解読して元データに復元して受信先の端末装置へ送信する手段を備えている。

【0041】したがって、上述の暗号化サーバS1、S2にネットワーク層のネットワークルーティング機能（ルータ）を設け、暗号化サーバS1はノードAの代理ARPをするノードとしての働きをする。

【0042】IPネットワークでは、1ネットワーク上に複数のルータが存在させることができ、実際の通信ではアドレス・リザリューション・プロトコル（ARP）によってIPアドレスから物理アドレス（MACアドレス）を求め、その物理アドレスで通信相手を指定して通信を行なう（データリンク層）。普通は、物理アドレスは通信相手が返してきたものを使用するが、別のノードがそれを返すこともできる。これを代理ARPと称する。

【0043】そして、各ネットワークにネットワークルータ機能と受信ノードの代わりにパケットを受け取る代理応答機能を備えた暗号化サーバを設ける。送信側のネットワークの送信ノードは、この暗号化サーバへ通信の秘密を守りたいデータのみを送り、暗号化サーバはそのデータを暗号化データに変換してネットワークルータ機能によってそのデータの受信先のネットワークへ送信する。

【0044】一方、受信側のネットワークの暗号化サー

バは、受信ノードの代わりにパケットを受け取る代理応答機能によって送信側ネットワークから送信されたパケット（暗号化データ）を受信し、それを解読して復元し、その復元されたデータを受信ノードへ送信する。

【0045】図3は、IPネットワークNET-1のノードAからIPネットワークNET-3のノードCへ暗号化通信を行なうときのデータの流れを示すフローチャートである。ここでは、暗号化サーバS1とS2の暗号化キー（キーコード）は固定されている場合について説明する。

【0046】ノードAは、初期化時、ローカルエリアネットワークの暗号化サーバS1のアドレスを登録し、その暗号化サーバS1を代理送受信するデフォルトルータとする。また、ノードCは、初期化時、ローカルエリアネットワークの暗号化サーバS2のアドレスを登録し、その暗号化サーバS2を代理送受信するデフォルトルータとする。

【0047】したがって、暗号化サーバS1はノードAの代理ARPとしてノードAへのデータを横取りし、同様に、暗号化サーバS2はノードCの代理ARPをするノードとして働き、ノードCへのデータを横取りする。

【0048】ノードAからノードCへのデータ送信時、ノードAは暗号化サーバS1に生データを送信する。暗号化サーバS1はその生データを暗号化後「暗号化済フラグ」を立ててルータR1へ転送する。その暗号化データは、ルータR1、R2、R3、R4の順番に転送されてノードCの代理ノードとしての暗号化サーバS2に転送される。

【0049】暗号化サーバS2はその暗号化データを受信して解読後、最後にノードCへ転送する。ノードCは暗号化サーバS2からノードAによって送信された暗号化データを復元されたデータで受け取る。

【0050】上記の第2実施例の暗号化サーバS1のルーティング機能は、受けたパケットを全てルータR1に渡すだけの機能が有れば十分であり、暗号化サーバS2のルーティング機能も、受けたパケットを全てルータR2に渡すだけの機能が有れば十分である。

【0051】このようにして、複数のネットワークにまたがるパケット通信の場合、すなわち外部のネットワークの受信先ノードへデータを出す場合、送信側のノードが暗号化サーバへ受信先ノードを指定して通信の秘密を守りたいデータを送信すれば、その暗号化サーバが直接受信先ノードのネットワークへ通信する。

【0052】したがって、送信側ノードは暗号化サーバにデータの暗号化を依頼して、暗号化されたデータを自ら受信先ノードへ送信することなく、暗号化サーバとのデータのやり取りを簡略化することができ、つまり、ノードと暗号化サーバとの1往復分のデータのやり取りの時間とトライフィックを節約でき、送信側ノードの処理負担を軽減し、データ通信の高速性及び効率性を図ること

ができる。

【0053】また、受信側ノードは、自己のネットワークに接続されている暗号化サーバによって送信側ノードから送信された暗号化データを復元された状態で受け取ることができるので、同様にノードと暗号化サーバとの1往復分のデータのやり取りの時間とトライフィックを節約でき、受信側ノードの処理負担を軽減し、データ通信の高速性及び効率性を図ることができる。

#### 【0054】

【発明の効果】以上説明してきたように、この発明によるローカルエリアネットワークによれば、ネットワークの各端末装置毎にデータの暗号化と復号化を行なわず、暗号化サーバによって集中して行なうので、各端末装置の処理負荷を軽減させることができ、ネットワークにおける暗号化キーの変更や暗号化方式の変更時にはその暗号化サーバの設定を変更するだけでよいので、それぞれの端末装置の設定を変更する煩雑な作業を行なわずに済み、ネットワークの管理を容易に行なえる。

【0055】また、外部のネットワークを介して複数のネットワーク間の端末装置間で通信を行なえるようにしたとき、データがどのようなネットワークの経路を通つて送受信されても途中で外部のものにデータ内容を覗かれてしまう危険がない。

【0056】さらに、ネットワークの各端末装置が、暗

号化サーバに対してデータの暗号化又はその解読に必要な暗号化キーを送信し、暗号化サーバが、各端末装置から受信した暗号化キーに基づいてデータの暗号化又はその解読を行なうようにすれば、多様な暗号化方式を容易に利用することができる。

#### 【図面の簡単な説明】

【図1】この発明の一実施例のローカルエリアネットワーク（LAN）のシステム構成を示す図である。

【図2】図1のノードAからノードCへ暗号化通信を行なうときのデータの流れを示すフローチャートである。

【図3】図1の暗号化サーバS1とS2のルーティング機能を用いてノードAからノードCへ暗号化通信を行なうときのデータの流れを示すフローチャートである。

【図4】各ノード間で送受信されるパケットのIPヘッダのフォーマットを示す図である。

【図5】図4のIPヘッダの「オプション（Options）」フィールドのフォーマットを示す図である。

#### 【符号の説明】

A～C：端末装置（ノード）

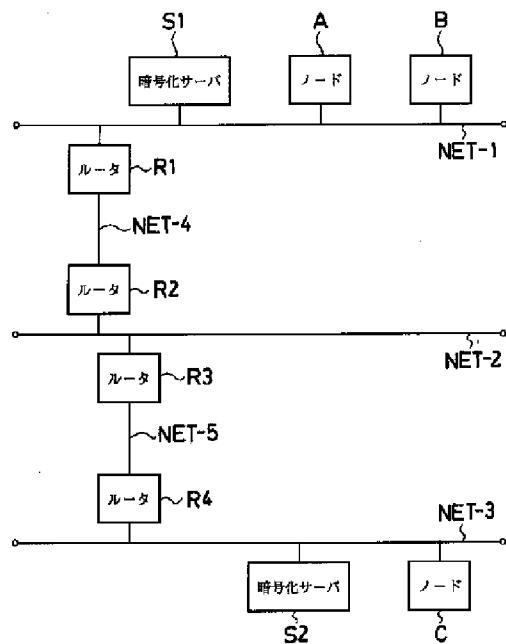
S1, S2：暗号化サーバ

R1～R4：ルータ

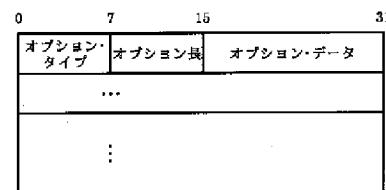
NET-1～NET-3：IPネットワーク

NET-4, NET-5：ネットワーク

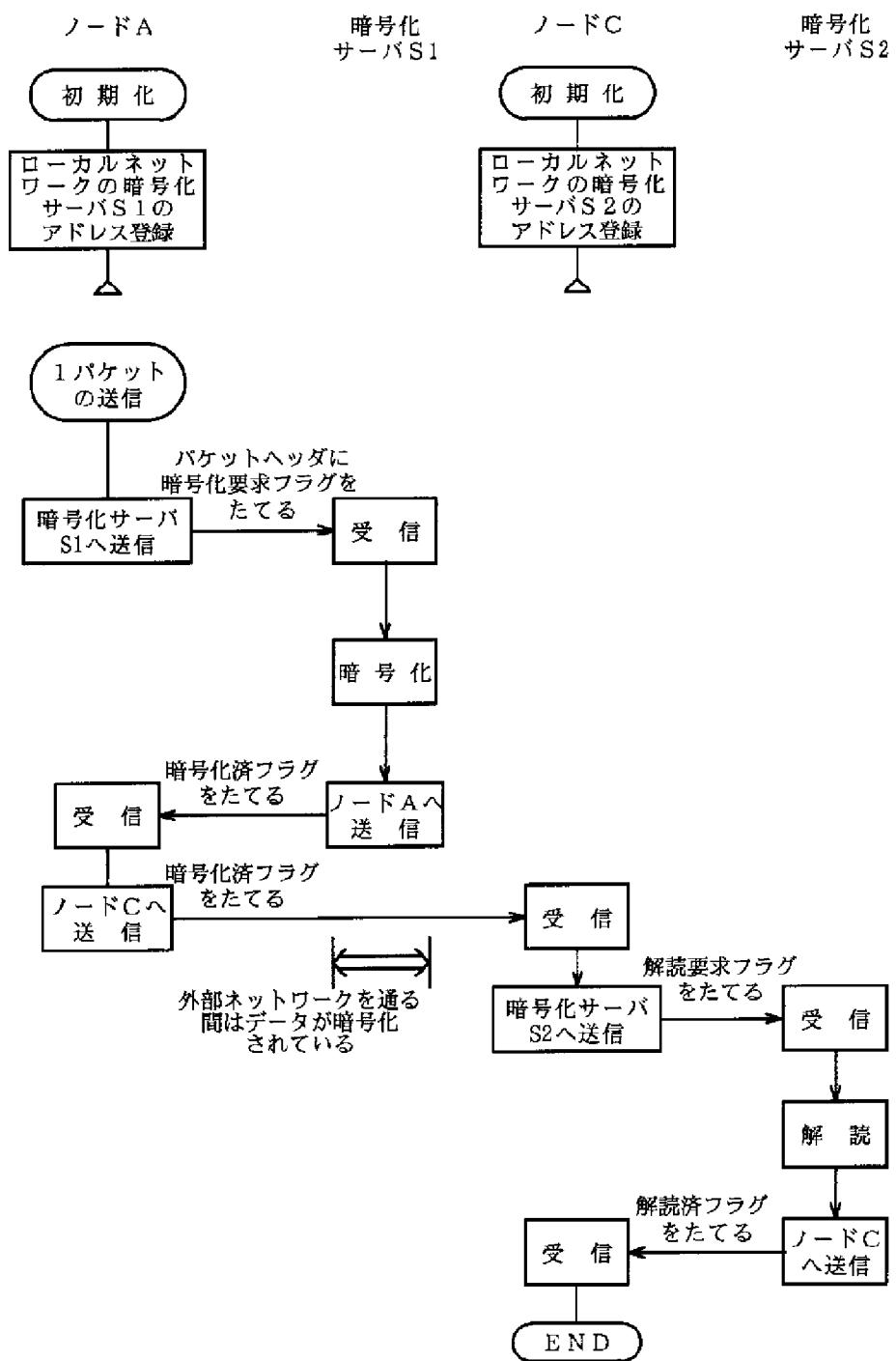
【図1】



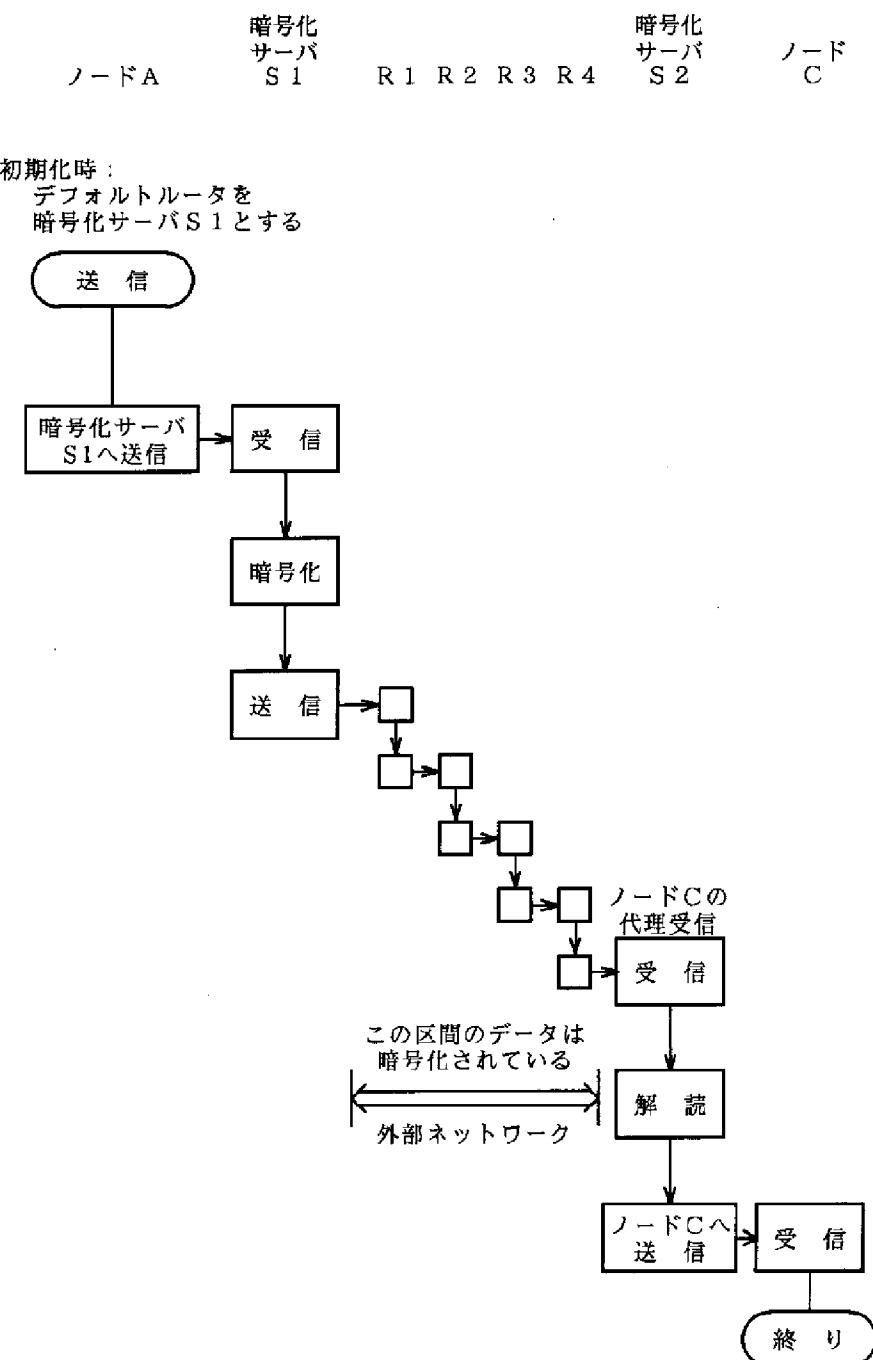
【図5】



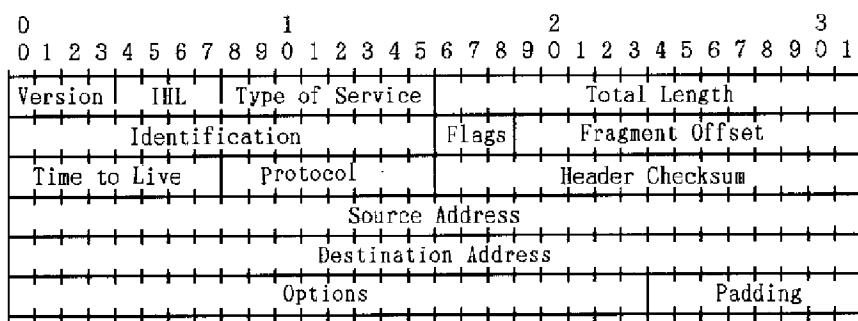
【図2】



【図3】



【図4】



---

フロントページの続き

(51) Int. Cl. <sup>6</sup>

識別記号

序内整理番号

F I

技術表示箇所

H 0 4 L 9/12

(54) [TITLE OF THE INVENTION] LOCAL AREA NETWORK

(57) [ABSTRACT]

[OBJECT] To enable data to be encrypted and transmitted/received between terminal devices without encrypting and decoding the data between the  
5 respective terminal devices.

[CONSTITUTION] An encryption server S1 converts original data transmitted from a node A as a terminal device of a transmitting source of an IP network NET-1 into encrypted data so as to return to the node A, and the node A transmits the encrypted data to a node C as a terminal device of a  
10 transmitting source of an IP network NET-3. On the other hand, an encryption server S2 decrypts and restores the encrypted data transmitted from the node C as the terminal device of a receiving destination of the IP network NET-3 into original data so as to return it to the node C.

[CLAIMS]

[Claim 1] A local area network where a plurality of terminal devices are connected by a network so that data can be transmitted/received between the terminal devices, the network comprising an encryption server having a unit for converting original data transmitted from the terminal device of a transmitting source into encrypted data so as to return it to the terminal device as the transmitting source, decrypting the encrypted data transmitted from the terminal device of a receiving destination and restoring it into the original data so as to return the original data to the terminal device of the receiving source.

[Claim 2] A local area network where a plurality of networks is connected so that data can be transmitted/received between a plurality of terminal devices, each of the networks comprising an encryption server having a unit for converting original data transmitted from a terminal device of a transmitting source into encrypted data so as to transmit the encrypted data to a terminal device of a receiving destination of different network, decrypting the encrypted data received from different network and restoring it into the original data so as to transmit the original data to the terminal device of the receiving destination.

[Claim 3] The local area network according to claim 1, wherein  
each of the terminal devices has a unit for transmitting an encryption key necessary for encrypting or decrypting data to the encryption server,  
the encryption server has a unit for encrypting or decrypting the data based on the encryption key received from each of the terminal devices.

[Detailed Description of the Invention]

[0001]

[Field of Industrial Application] The present invention relates to a local area

network for connecting a plurality of terminal devices via the network.

[0002]

[Prior Art] Conventionally, in a local area network (hereinafter, “LAN”) complying with standards of Ethernet or IEEE802.3, in order to keep secret of 5 the contents of packets transmitted/received between respective terminal devices (hereinafter, “nodes”), the contents of the packets to be transmitted from on a node on a transmitting side are encrypted by a predetermined encryption system so as to be transmitted to a node of a destination node, and the received and encrypted packets are decrypted and restored into original 10 data contents on the node on receiving side of the destination.

[0003] The encryption system is a technique that converts information understandable by anybody into meaningless code texts based on a predetermined encryption key (simply “key”), and decrypts the code texts using the same encryption key used in the encryption so as to restore them 15 into the original information (referred to as “decoding”).

[0004] In general, a common key encryption system such as a DES encryption method and an FEAL encryption method complying with standard encryption are known as the encryption system. In the common key encryption system, identical encryption key and decoding key are shared between transmitters 20 and receivers, and data are encrypted and decoded (restored) by using the common key.

[0005]

[Problem to be Solved by the Invention] However, since the encryption of 25 packets for keeping communication secrets is not standardized in the above conventional LAN, the contents of the packets should be encrypted at a node on a transmitting side so as to be transmitted, and the encrypted data contents of the received packets should be decrypted so as to be restored into

the original data at a node on a receiving sides.

[0006] Therefore, a processing load is put on the respective nodes, and further when the encryption key and the encryption system (decryption method) are changed, the settings of all the nodes on LAN should be changed. This is very

5 inconvenient.

[0007] Further, in a local network environment, since a network is in a managed state or is easily managed, reliability of the network is high.

However, communication is enabled between a plurality of terminal devices in a plurality of networks via an external network, routes of networks through

10 which data are transmitted/received and reach a destination cannot be obtained. For this reason, there arises a problem that the data contents may be intercepted by outsiders on such routes.

[0008] The present invention is devised in view of the above point, and its object is to enable data to be encrypted and transmitted/received between

15 terminal devices without encrypting and decoding in the respective terminal devices.

[0009]

[Means for Solving the Problem] In order to achieve the above object, the present invention provides a local area network where a plurality of terminal

20 devices is connected by a network so that data can be transmitted/received between the terminal devices, the network comprising an encryption server having a unit for converting original data transmitted from the terminal

device of a transmitting source into encrypted data so as to return it to the terminal device as the transmitting source, decrypting the encrypted data

25 transmitted from the terminal device of a receiving destination and restoring it into the original data so as to return the original data to the terminal device of the receiving source.

[0010] Further, the invention provides a local area network where a plurality of networks is connected so that data can be transmitted/received between a plurality of terminal devices, each of the networks comprising an encryption server having a unit for converting original data transmitted from a terminal device of a transmitting source into encrypted data so as to transmit the encrypted data to a terminal device of a receiving destination of different network, decrypting the encrypted data received from different network and restoring it into the original data so as to transmit the original data to the terminal device of the receiving destination.

5

[0011] Further, in the above local area network, each of the terminal devices has a unit for transmitting an encryption key necessary for encrypting or decrypting data to the encryption server, and the encryption server has a unit for encrypting or decrypting the data based on the encryption key received from each of the terminal devices.

10

[0012]

[Function] In the local area network of the present invention, the encryption server provided to the network converts original data transmitted from the terminal device of the transmitting source into encrypted data and returns it to the terminal device of the transmitting source, decrypts the encrypted data transmitted from the terminal device of the receiving destination so as to restore it into the original data, and returns the original data to the terminal device of the receiving destination. For this reason, the data can be encrypted and transmitted/received between the terminal devices without encrypting and decrypting the data in the respective terminal devices.

15

[0013] Further, each of the encryption servers provided to a plurality of connected networks convert original data transmitted from the terminal device of the transmitting source into encrypted data so as to transmit it to a

20

25

terminal device of the receiving destination in different network, and decrypts the encrypted data received from the different network so as to restore it into the original data, and transmits the original data to the terminal device of the receiving destination. For this reason, the data can be encrypted and

5 transmitted/received between terminal devices in the respective networks without encrypting and decoding the data in the respective terminal devices.

[0014] Further, each of the terminal devices transmits an encryption key necessary for encrypting and decrypting data to the encryption server, the encryption server encrypts or decrypts the data based on the encryption key 10 received from each of the terminal devices. As a result, the encryption and decoding can be performed according to the encryption method based on the encryption key.

[0015]

[Embodiments] Embodiments of the present invention are described

15 concretely below with reference to drawings. Fig. 1 is a diagram illustrating a system structure of a local area network (LAN) according to one embodiment of the present invention. This local area network uses a TCP/IP protocol. This local area network includes three IP networks NET-1, NET-2 and NET-3.

20 [0016] The IP network NET-1 is connected to terminal devices (nodes) A and B containing a microcomputer composed of CPU, ROM and RAM, and is connected to an encryption server S1 that is one kind of a terminal device having a microcomputer and encrypts and decrypts (restores) data of the nodes A and B, and is connected to a router (referred to as “gateway”) R1 for 25 routing a packet between two networks.

[0017] Further, the IP network NET-2 is connected to routers R2 and R3 for routing a packet between two networks. Further, the IP network NET-3 is

connected to a node C containing a microcomputer, and is connected to an encryption server S2 that is one kind of a terminal device containing a microcomputer and encrypts and decrypts (restores) data of the node C. The IP network NET-3 is connected to a router R4 for routing a packet between  
5 two networks.

[0018] The routers R1 and R2 are connected by a network NET-4, and the routers R3 and R4 are connected by a network NET-5, so that data can be transmitted/received between the nodes A, B and C of the IP networks NET-1 and NET-3. At this time, the encryption servers S1 and S2 can encrypt the  
10 data and can decode the received encrypted data (referred to as “encrypted communication”).

[0019] The encryption servers S1 and S2 have a unit for converting original data transmitted from a terminal device of a transmitting source into encrypted data so as to return the encrypted data to the terminal device of the transmitting source, and decrypting the encrypted data transmitted from a terminal device of a receiving destination and restoring it into the original data so as to return the original data to the terminal device of the receiving destination. In this case, the same encryption key and the same encryption algorithm are used for the encryption and the decryption.  
15

20 [0020] Fig. 2 is a flowchart illustrating a flow of data when encrypted communication is held from the node A of the IP network NET-1 to the node C of the IP network NET-3. The case where an encryption key (key code) of the encryption servers S1 and S2 is fixed is described.

[0021] At first, at the time of initialization, the node A registers an address of  
25 the encryption server S1 in the local area network, and the node C registers an address of the encryption server S2 in the local area network.

[0022] When transmission for one packet is requested, the node A sets an

“encryption request flag” for the encryption server S1, so as to transmit raw data. The encryption server S1 encrypts the raw data received from the node A using an encryption key according to a preset encryption method, and sets an “encrypted flag” so as to return the data to the node A.

- 5 [0023] The node A adds information representing the encrypted data to the encrypted data received from the encryption server S1, and transmits (transfers) the encrypted data to the node C of the IP network NET-3. The information representing the encrypted data may be stored in a header section of the packet.
- 10 [0024] On the other hand, the node C checks the header section of the packet received from the node A, and when the information representing the encrypted data is stored, it determines that the packet is the encrypted data. The node C sets a “decryption request flag” for the encrypted data, and transfers the encrypted data to the encryption server S2. The encryption server S2 decrypts and restores the encrypted data received from the node C using the encryption key, and sets a “decrypted flag” so as to return the restored data to the node C. The node C acquires the restored data from the encryption server S2.
- 15 [0025] In such a manner, the encryption servers for encrypting and decrypting data are provided to respective networks, and the encryption servers collectively encrypt and decrypt data transmitted/received to/from the respective terminal devices on the networks. For this reason, each of the respective terminal devices does not have to encrypt and decrypt the data.
- 20 [0026] Fig. 4 is a diagram illustrating a format of the IP header of the packet, and Fig. 5 is a diagram illustrating a format of an “Options” field of the IP header. The encryption request flag, the encrypted flag, the decryption request flag and the decrypted flag are defined on an option area of the

“Options” field of the IP header.

[0027] Table 1 is a table illustrating one example of option data, and respective flags are, for example, the encryption request flag “0”, the encrypted flag “1”, the decryption request flag “3” and the decrypted flag “4”.

5 [0028]

[Table 1]

Class	Number	Length	Function
0	0	1	End of Option List
0	1	1	NOP (No Operation)
0	2	11	Restriction on Security and Process
0	3	Variable	Loose Source Routing
0	9	Variable	String Source Routing
0	7	Variable	Record Route
0	8	4	Stream Identifier
2	4	Variable	Time Stamp
1	1	1	Flag 0: Encryption Request 1: Decryption Request 2: Encrypted 3: Decrypted

[0029] An example where when the encrypted communication is held from the node A of the IP network NET-1 to the node C of the IP network NET-3, an encryption key for encrypting and decrypting data is transmitted to the

10 encryption servers S1 and S2 is described below.

[0030] In this case, the nodes A and C have a function for transmitting the encryption key for encrypting or decrypting data to the encryption servers S1

and S2. The encryption servers S1 and S2 have a function for performing the encryption and decryption methods using a plurality of encryption keys, and they encrypt and decrypt data using the encryption keys transmitted from the nodes A and C.

5 [0031] At first, the node A holds initialization communication that standardizes an encryption key necessary for exchanging encrypted data with the node C. This initialization communication provides the encryption key of the same encryption method to the nodes A and C.

10 [0032] When original data is transmitted from the node A to the encryption server S1, the encryption key is attached, and the encryption server S1 encrypts the original data using the encryption key. Further, at the time of decrypting the encrypted data, the node C attaches the encryption key when requesting the encryption server S2 to decrypt the encrypted data, and the encryption server S2 restores the encrypted data using the encryption key.

15 The encryption key is defined in "option data" of the IP header shown in Figs. 4 and 5, for example.

20 [0033] When transmission request of one packet is generated, the node A sets the "encryption request flag" for the encryption server S1, and transmits raw data together with the encryption key. The encryption server S1 encrypts the raw data received from the node A according the encryption method using the encryption key, sets the "encrypted flag" and returns the data to the node A. The node A transmits (transfers) the encrypted data received from the encryption server S1 to the node C of the IP network NET-3.

25 [0034] On the other hand, when the node C receives the encrypted data from the node A, it sets the "decryption request flag" and transmits the encrypted data as well as the encryption key to the encryption server S2. The encryption server S2 restores the encrypted data received from the node C

according to the decryption method using the encryption key, and sets the "decrypted flag" so as to return the restored data to the node C. The node C obtains the restored data from the encryption server S2. Therefore, in this LAN, a key code is variable.

5 [0035] An example, that when the encrypted communication is held from node A of the IP network NET-1 to the node B, the encryption key for encrypting and decrypting data is transmitted to the encryption server S1, is described below.

[0036] When transmission request for one packet is generated, the node A sets 10 the "encryption request flag" for the encryption server S1, and transmits raw data as well as an encryption key. The encryption server S1 encrypts the raw data received from the node A according to the encryption method using the encryption key, and sets the "encrypted flag" so as to return the data to the node A. The node A transmits (transfers) the encrypted data received from 15 the encryption server S1 to the node B.

[0037] On the other hand, when the node B receives the encrypted data from the node A, it sets the "decryption request flag" and transfers the encrypted data as well as the encryption key to the encryption server S1. The encryption server S1 restores the encrypted data received from node B 20 according to the decryption method using the encryption key, and sets the "decrypted flag" so as to return the restored data to the node B. The node B obtains the restored data from the encryption server S1.

[0038] In such a manner, when each terminal device requests the encryption server to encrypt and decrypt data, each of them transmits the encryption key 25 necessary for the encryption and decryption together with the data, and the encryption server encrypts and decrypts the data according to the encryption method using the encryption key. For this reason, each of the terminal

devices can easily utilize the data transmission/reception according to various encryption methods. Further, since each node can freely set an encryption key and can select the encryption method for data, the secrecy of the data communication can be further heightened.

5 [0039] An example of the encrypted communication when a network routing function is provided to the encryption server is described below. The network structure in this case is the same as that of the local area network shown in Fig. 1, but the functions of the nodes A, B and C and the encryption servers S1 and S2 are slightly different.

10 [0040] The encryption servers S1 and S2 in this example has a unit for converting original data transmitted from the terminal device of the transmitting source into encrypted data so as to transmit the encrypted data to the terminal device of the receiving destination in different network, and decrypting the encrypted data received from another network so as to restore 15 it into the original data and transmit it to the terminal device of the receiving destination.

[0041] Therefore, a network routing function (router) of a network layer is provided to the encryption servers S1 and S2, and the encryption server S1 functions as a node that is a substitute for the node A at which ARP is 20 implemented.

[0042] In an IP network, a plurality of routers can be provided to one network, and in actual communication, a physical address (MAC address) is obtained from an IP address according to an address resolution protocol (ARP), and a communication destination is specified by the physical address so that 25 communication is held (data link layer). Normally, the physical address that is returned from the communication destination is used, but a different node can return it. This is called as the substitute ARP.

[0043] Each network is provided with an encryption server having a network router function and a substitute response function for receiving a packet instead of a receiving node. A transmitting node of the network on a transmitting side sends only data whose communication secret is desired to be kept to the encryption server, and encryption server converts the data into the encrypted data so as to transmit the data to a network of a receiving destination of this data using the network router function.

5 [0044] On the other hand, the encryption server of the network on the receiving side receives the packet (encrypted data) transmitted from the network on the transmitting side using the substitute response function for receiving the packet instead of the receiving node, and restores the packet so as to transmit the restored data to the receiving node.

10 [0045] Fig. 3 is a flow chart illustrating a flow of data when the encrypted communication is held between the node A of the IP network NET-1 to the node C of the IP network NET-3. The case where an encryption key (key code) of the encryption servers S1 and S2 is fixed is described.

15 [0046] The node A registers an address of the encryption server S1 of the local area network at the time of initialization, and the encryption server S1 is used as a default router for carrying out substitute transmission/reception.

20 Further, the node C registers an address of the encryption server S2 of the local area network at the time of initialization, and the encryption server S2 is used as a default router for carrying out substitute transmission/reception.

25 [0047] Therefore, the encryption server S1 intercepts the data to be transmitted to the node A as the substitute ARP of the node A, and similarly the encryption server S2 functions as the node for implementing the substitute ARP of the node C to intercept the data to be transmitted to the node C.

[0048] At the time of the data transmission from the node A to the node C, the node A transmits raw data to the encryption server S1. The encryption server S1 encrypts the raw data and sets the "encrypted flag" so as to transmit the encrypted data to the router R1. The encrypted data is transmitted to the routers R1, R2, R3 and R4 in this order, and then to the encryption server S2 substitute for the node C.

[0049] The encryption server S2 receives and decrypts the encrypted data, and finally transmits it to the node C. The node C receives the encrypted data transmitted by the node A from the encryption server S2 as the restored data.

10 [0050] As to the routing function of the encryption server S1 according to the second embodiment, it is only necessary to transmit all received packets to the router R1. As to the routing function of the encryption server S2, it is only necessary to transmit all received packets to the router R2.

15 [0051] In such a manner, in the case of the packet communication between a plurality of networks, namely, in the case where data is sent to a receiving destination node of an external network, when the node on the transmitting side specifies the receiving destination node and transmits data whose communication secret is desired to be kept to the encryption server, the encryption server directly communicates with the network of the receiving destination node.

20 [0052] Therefore, the node on the transmitting side does neither request the encryption server to encrypt data nor transmit the encrypted data to the receiving destination node, so that the exchange of the data with the encryption server can be simplified. That is to say, the time and traffic for 25 one reciprocation required for exchanging the data between the node and the encryption server can be saved, and the processing load on the node on the transmitting side can be reduced, thereby securing the high-speed

performance and efficiency of the data communication.

[0053] The node on the receiving side can receive the encrypted data transmitted from the node on the transmitting side by the encryption server connected to a self network as the restored data. For this reason, the time and traffic for one reciprocation required for exchanging the data between the node and the encryption server can be saved similarly, and the processing load put on the node on the receiving side can be saved, thereby securing the high-speed performance and efficiency of the data communication.

[0054]

10 [Effect of the Invention] As described above, in the local area network according to the present invention, the encryption and decoding of data are performed not by each terminal device of the network but by the encryption server in a centralized manner. For this reason, the processing load put on each terminal device can be reduced, and it is only necessary to change the 15 settings of the encryption server at the time of changing the encryption key and the encryption method in the network. As a result, a complicated operation for changing the settings of each terminal device does not have to be performed, and thus the network can be easily managed.

20 [0055] When the communication can be held between the terminal devices in a plurality of networks via an external network, even if data is transmitted/received through any network routes, the data contents are not in danger of being intercepted by outsiders on such routes.

25 [0056] Further, each terminal device in the networks transmits an encryption key necessary for the encryption or decryption of data to the encryption server, and the encryption server encrypts or decrypts the data based on the encryption key received from each terminal device, so that various encryption methods can be easily utilized.

[Brief Description of the Drawings]

[Fig. 1] Fig. 1 is a diagram illustrating a system structure of a local area network (LAN) according to one embodiment of the present invention.

[Fig. 2] Fig. 2 is a flowchart illustrating a flow of data when encrypted

5 communication is held from a node A to a node C in Fig. 1.

[Fig. 3] Fig. 3 is a flowchart illustrating a flow of data when the encrypted communication is held from the node A to node C by using a routing function of encryption servers S1 and S2 in Fig. 1.

[Fig. 4] Fig. 4 is a diagram illustrating a format of an IP header of a packet

10 transmitted/received between the nodes.

[Fig. 5] Fig. 5 is a diagram illustrating a format of an “Options” field of the IP header.

[Explanations of Letters or Numerals]

A to C: terminal device (node)

15 S1, S2: encryption server

R1 to R4: Router

NET-1 to NET-3: IP network

NET-4, NET-5: network

20 FIG. 1

1: ENCRYPTION SERVER

2: NODE

3: ROUTER

FIG. 5

25 1: OPTION TYPE

2: OPTION LENGTH

3: OPTION DATA

FIG. 2

- 1: NODE A
- 2: ENCRYPTION SERVER S1
- 3: NODE C
- 5 4: INITIALIZE
- 5: REGISTER ADDRESS OF ENCRYPTION SERVER S2 OF LOCAL NETWORK
- 6: ENCRYPTION SERVER S2
- 7: INITIALIZE
- 10 8: REGISTER ADDRESS OF ENCRYPTION SERVER S1 OF LOCAL NETWORK
- 9: TRANSMIT ONE PACKET
- 10: SET ENCRYPTION REQUEST FLAG FOR PACKET HEADER
- 11: TRANSMIT TO ENCRYPTION SERVER S1
- 15 12: RECEIVE
- 13: ENCRYPT
- 14: SET ENCRYPTED FLAG
- 15: TRANSMIT TO NODE A
- 16: TRANSMIT TO NODE C
- 20 17: WHILE PASSING THROUGH EXTERNAL NETWORK, DATA IS BEING ENCRYPTED.
- 18: TRANSMIT TO ENCRYPTION SERVER S2
- 19: SET DECRYPTION REQUEST FLAG
- 20: DECRYPT
- 25 21: SET DECRYPTED FLAG
- 22: TRANSMIT TO NODE C

FIG. 3

- 1: NODE A
- 2: ENCRYPTION SERVER S1
- 3: ENCRYPTION SERVER S2
- 4: NODE C
- 5: 5: AT THE TIME OF INITIALIZATION: USE DEFAULT ROUTER AS ENCRYPTION SERVER S1
- 6: TRANSMIT
- 7: TRANSMIT TO ENCRYPTION SERVER S1
- 8: RECEIVE
- 10 9: ENCRYPT
- 10: SUBSTITUTE RECEPTION OF NODE C
- 11: DATA IN THIS ZONE IS ENCRYPTED.
- 12: EXTERNAL NETWORK
- 13: DECRYPT
- 15 14: TRANSMIT TO NODE C
- 15: END

(54) [TITLE OF THE INVENTION] LOCAL AREA NETWORK

(57) [ABSTRACT]

[OBJECT] To enable data to be encrypted and transmitted/received between terminal devices without encrypting and decoding the data between the 5 respective terminal devices.

[CONSTITUTION] An encryption server S1 converts original data transmitted from a node A as a terminal device of a transmitting source of an IP network NET-1 into encrypted data so as to return to the node A, and the node A transmits the encrypted data to a node C as a terminal device of a 10 transmitting source of an IP network NET-3. On the other hand, an encryption server S2 decrypts and restores the encrypted data transmitted from the node C as the terminal device of a receiving destination of the IP network NET-3 into original data so as to return it to the node C.

[CLAIMS]

[Claim 1] A local area network where a plurality of terminal devices are connected by a network so that data can be transmitted/received between the terminal devices, the network comprising an encryption server having a unit for converting original data transmitted from the terminal device of a transmitting source into encrypted data so as to return it to the terminal device as the transmitting source, decrypting the encrypted data transmitted from the terminal device of a receiving destination and restoring it into the original data so as to return the original data to the terminal device of the receiving source.

[Claim 2] A local area network where a plurality of networks is connected so that data can be transmitted/received between a plurality of terminal devices, each of the networks comprising an encryption server having a unit for converting original data transmitted from a terminal device of a transmitting source into encrypted data so as to transmit the encrypted data to a terminal device of a receiving destination of different network, decrypting the encrypted data received from different network and restoring it into the original data so as to transmit the original data to the terminal device of the receiving destination.

[Claim 3] The local area network according to claim 1, wherein  
each of the terminal devices has a unit for transmitting an encryption key necessary for encrypting or decrypting data to the encryption server,  
the encryption server has a unit for encrypting or decrypting the data based on the encryption key received from each of the terminal devices.

[Detailed Description of the Invention]

[0001]

[Field of Industrial Application] The present invention relates to a local area

network for connecting a plurality of terminal devices via the network.

[0002]

[Prior Art] Conventionally, in a local area network (hereinafter, “LAN”) complying with standards of Ethernet or IEEE802.3, in order to keep secret of

5 the contents of packets transmitted/received between respective terminal devices (hereinafter, “nodes”), the contents of the packets to be transmitted from on a node on a transmitting side are encrypted by a predetermined encryption system so as to be transmitted to a node of a destination node, and the received and encrypted packets are decrypted and restored into original 10 data contents on the node on receiving side of the destination.

[0003] The encryption system is a technique that converts information understandable by anybody into meaningless code texts based on a predetermined encryption key (simply “key”), and decrypts the code texts using the same encryption key used in the encryption so as to restore them 15 into the original information (referred to as “decoding”).

[0004] In general, a common key encryption system such as a DES encryption method and an FEAL encryption method complying with standard encryption are known as the encryption system. In the common key encryption system, identical encryption key and decoding key are shared between transmitters 20 and receivers, and data are encrypted and decoded (restored) by using the common key.

[0005]

[Problem to be Solved by the Invention] However, since the encryption of packets for keeping communication secrets is not standardized in the above 25 conventional LAN, the contents of the packets should be encrypted at a node on a transmitting side so as to be transmitted, and the encrypted data contents of the received packets should be decrypted so as to be restored into

the original data at a node on a receiving sides.

[0006] Therefore, a processing load is put on the respective nodes, and further when the encryption key and the encryption system (decryption method) are changed, the settings of all the nodes on LAN should be changed. This is very

5 inconvenient.

[0007] Further, in a local network environment, since a network is in a managed state or is easily managed, reliability of the network is high. However, communication is enabled between a plurality of terminal devices in a plurality of networks via an external network, routes of networks through

10 which data are transmitted/received and reach a destination cannot be obtained. For this reason, there arises a problem that the data contents may be intercepted by outsiders on such routes.

[0008] The present invention is devised in view of the above point, and its object is to enable data to be encrypted and transmitted/received between

15 terminal devices without encrypting and decoding in the respective terminal devices.

[0009]

[Means for Solving the Problem] In order to achieve the above object, the present invention provides a local area network where a plurality of terminal

20 devices is connected by a network so that data can be transmitted/received between the terminal devices, the network comprising an encryption server having a unit for converting original data transmitted from the terminal device of a transmitting source into encrypted data so as to return it to the terminal device as the transmitting source, decrypting the encrypted data

25 transmitted from the terminal device of a receiving destination and restoring it into the original data so as to return the original data to the terminal device of the receiving source.

[0010] Further, the invention provides a local area network where a plurality of networks is connected so that data can be transmitted/received between a plurality of terminal devices, each of the networks comprising an encryption server having a unit for converting original data transmitted from a terminal device of a transmitting source into encrypted data so as to transmit the encrypted data to a terminal device of a receiving destination of different network, decrypting the encrypted data received from different network and restoring it into the original data so as to transmit the original data to the terminal device of the receiving destination.

5

[0011] Further, in the above local area network, each of the terminal devices has a unit for transmitting an encryption key necessary for encrypting or decrypting data to the encryption server, and the encryption server has a unit for encrypting or decrypting the data based on the encryption key received from each of the terminal devices.

10

[0012]

[Function] In the local area network of the present invention, the encryption server provided to the network converts original data transmitted from the terminal device of the transmitting source into encrypted data and returns it to the terminal device of the transmitting source, decrypts the encrypted data transmitted from the terminal device of the receiving destination so as to restore it into the original data, and returns the original data to the terminal device of the receiving destination. For this reason, the data can be encrypted and transmitted/received between the terminal devices without encrypting and decrypting the data in the respective terminal devices.

15

[0013] Further, each of the encryption servers provided to a plurality of connected networks convert original data transmitted from the terminal device of the transmitting source into encrypted data so as to transmit it to a

20

25

terminal device of the receiving destination in different network, and decrypts the encrypted data received from the different network so as to restore it into the original data, and transmits the original data to the terminal device of the receiving destination. For this reason, the data can be encrypted and

5 transmitted/received between terminal devices in the respective networks without encrypting and decoding the data in the respective terminal devices.

[0014] Further, each of the terminal devices transmits an encryption key necessary for encrypting and decrypting data to the encryption server, the encryption server encrypts or decrypts the data based on the encryption key 10 received from each of the terminal devices. As a result, the encryption and decoding can be performed according to the encryption method based on the encryption key.

[0015]

[Embodiments] Embodiments of the present invention are described

15 concretely below with reference to drawings. Fig. 1 is a diagram illustrating a system structure of a local area network (LAN) according to one embodiment of the present invention. This local area network uses a TCP/IP protocol. This local area network includes three IP networks NET-1, NET-2 and NET-3.

20 [0016] The IP network NET-1 is connected to terminal devices (nodes) A and B containing a microcomputer composed of CPU, ROM and RAM, and is connected to an encryption server S1 that is one kind of a terminal device having a microcomputer and encrypts and decrypts (restores) data of the nodes A and B, and is connected to a router (referred to as “gateway”) R1 for 25 routing a packet between two networks.

[0017] Further, the IP network NET-2 is connected to routers R2 and R3 for routing a packet between two networks. Further, the IP network NET-3 is

connected to a node C containing a microcomputer, and is connected to an encryption server S2 that is one kind of a terminal device containing a microcomputer and encrypts and decrypts (restores) data of the node C. The IP network NET-3 is connected to a router R4 for routing a packet between  
5 two networks.

[0018] The routers R1 and R2 are connected by a network NET-4, and the routers R3 and R4 are connected by a network NET-5, so that data can be transmitted/received between the nodes A, B and C of the IP networks NET-1 and NET-3. At this time, the encryption servers S1 and S2 can encrypt the  
10 data and can decode the received encrypted data (referred to as “encrypted communication”).

[0019] The encryption servers S1 and S2 have a unit for converting original data transmitted from a terminal device of a transmitting source into encrypted data so as to return the encrypted data to the terminal device of the transmitting source, and decrypting the encrypted data transmitted from a terminal device of a receiving destination and restoring it into the original data so as to return the original data to the terminal device of the receiving destination. In this case, the same encryption key and the same encryption algorithm are used for the encryption and the decryption.  
15

20 [0020] Fig. 2 is a flowchart illustrating a flow of data when encrypted communication is held from the node A of the IP network NET-1 to the node C of the IP network NET-3. The case where an encryption key (key code) of the encryption servers S1 and S2 is fixed is described.

25 [0021] At first, at the time of initialization, the node A registers an address of the encryption server S1 in the local area network, and the node C registers an address of the encryption server S2 in the local area network.

[0022] When transmission for one packet is requested, the node A sets an

“encryption request flag” for the encryption server S1, so as to transmit raw data. The encryption server S1 encrypts the raw data received from the node A using an encryption key according to a preset encryption method, and sets an “encrypted flag” so as to return the data to the node A.

- 5 [0023] The node A adds information representing the encrypted data to the encrypted data received from the encryption server S1, and transmits (transfers) the encrypted data to the node C of the IP network NET-3. The information representing the encrypted data may be stored in a header section of the packet.
- 10 [0024] On the other hand, the node C checks the header section of the packet received from the node A, and when the information representing the encrypted data is stored, it determines that the packet is the encrypted data. The node C sets a “decryption request flag” for the encrypted data, and transfers the encrypted data to the encryption server S2. The encryption server S2 decrypts and restores the encrypted data received from the node C using the encryption key, and sets a “decrypted flag” so as to return the restored data to the node C. The node C acquires the restored data from the encryption server S2.
- 15 [0025] In such a manner, the encryption servers for encrypting and decrypting data are provided to respective networks, and the encryption servers collectively encrypt and decrypt data transmitted/received to/from the respective terminal devices on the networks. For this reason, each of the respective terminal devices does not have to encrypt and decrypt the data.
- 20 [0026] Fig. 4 is a diagram illustrating a format of the IP header of the packet, and Fig. 5 is a diagram illustrating a format of an “Options” field of the IP header. The encryption request flag, the encrypted flag, the decryption request flag and the decrypted flag are defined on an option area of the

“Options” field of the IP header.

[0027] Table 1 is a table illustrating one example of option data, and respective flags are, for example, the encryption request flag “0”, the encrypted flag “1”, the decryption request flag “3” and the decrypted flag “4”.

5 [0028]

[Table 1]

Class	Number	Length	Function
0	0	1	End of Option List
0	1	1	NOP (No Operation)
0	2	11	Restriction on Security and Process
0	3	Variable	Loose Source Routing
0	9	Variable	String Source Routing
0	7	Variable	Record Route
0	8	4	Stream Identifier
2	4	Variable	Time Stamp
1	1	1	Flag 0: Encryption Request 1: Decryption Request 2: Encrypted 3: Decrypted

[0029] An example where when the encrypted communication is held from the node A of the IP network NET-1 to the node C of the IP network NET-3, an encryption key for encrypting and decrypting data is transmitted to the

10 encryption servers S1 and S2 is described below.

[0030] In this case, the nodes A and C have a function for transmitting the encryption key for encrypting or decrypting data to the encryption servers S1

and S2. The encryption servers S1 and S2 have a function for performing the encryption and decryption methods using a plurality of encryption keys, and they encrypt and decrypt data using the encryption keys transmitted from the nodes A and C.

5 [0031] At first, the node A holds initialization communication that standardizes an encryption key necessary for exchanging encrypted data with the node C. This initialization communication provides the encryption key of the same encryption method to the nodes A and C.

10 [0032] When original data is transmitted from the node A to the encryption server S1, the encryption key is attached, and the encryption server S1 encrypts the original data using the encryption key. Further, at the time of decrypting the encrypted data, the node C attaches the encryption key when requesting the encryption server S2 to decrypt the encrypted data, and the encryption server S2 restores the encrypted data using the encryption key.

15 The encryption key is defined in "option data" of the IP header shown in Figs. 4 and 5, for example.

20 [0033] When transmission request of one packet is generated, the node A sets the "encryption request flag" for the encryption server S1, and transmits raw data together with the encryption key. The encryption server S1 encrypts the raw data received from the node A according the encryption method using the encryption key, sets the "encrypted flag" and returns the data to the node A. The node A transmits (transfers) the encrypted data received from the encryption server S1 to the node C of the IP network NET-3.

25 [0034] On the other hand, when the node C receives the encrypted data from the node A, it sets the "decryption request flag" and transmits the encrypted data as well as the encryption key to the encryption server S2. The encryption server S2 restores the encrypted data received from the node C

according to the decryption method using the encryption key, and sets the "decrypted flag" so as to return the restored data to the node C. The node C obtains the restored data from the encryption server S2. Therefore, in this LAN, a key code is variable.

5 [0035] An example, that when the encrypted communication is held from node A of the IP network NET-1 to the node B, the encryption key for encrypting and decrypting data is transmitted to the encryption server S1, is described below.

[0036] When transmission request for one packet is generated, the node A sets 10 the "encryption request flag" for the encryption server S1, and transmits raw data as well as an encryption key. The encryption server S1 encrypts the raw data received from the node A according to the encryption method using the encryption key, and sets the "encrypted flag" so as to return the data to the node A. The node A transmits (transfers) the encrypted data received from 15 the encryption server S1 to the node B.

[0037] On the other hand, when the node B receives the encrypted data from the node A, it sets the "decryption request flag" and transfers the encrypted data as well as the encryption key to the encryption server S1. The encryption server S1 restores the encrypted data received from node B 20 according to the decryption method using the encryption key, and sets the "decrypted flag" so as to return the restored data to the node B. The node B obtains the restored data from the encryption server S1.

[0038] In such a manner, when each terminal device requests the encryption server to encrypt and decrypt data, each of them transmits the encryption key 25 necessary for the encryption and decryption together with the data, and the encryption server encrypts and decrypts the data according to the encryption method using the encryption key. For this reason, each of the terminal

devices can easily utilize the data transmission/reception according to various encryption methods. Further, since each node can freely set an encryption key and can select the encryption method for data, the secrecy of the data communication can be further heightened.

5 [0039] An example of the encrypted communication when a network routing function is provided to the encryption server is described below. The network structure in this case is the same as that of the local area network shown in Fig. 1, but the functions of the nodes A, B and C and the encryption servers S1 and S2 are slightly different.

10 [0040] The encryption servers S1 and S2 in this example has a unit for converting original data transmitted from the terminal device of the transmitting source into encrypted data so as to transmit the encrypted data to the terminal device of the receiving destination in different network, and decrypting the encrypted data received from another network so as to restore 15 it into the original data and transmit it to the terminal device of the receiving destination.

[0041] Therefore, a network routing function (router) of a network layer is provided to the encryption servers S1 and S2, and the encryption server S1 functions as a node that is a substitute for the node A at which ARP is 20 implemented.

[0042] In an IP network, a plurality of routers can be provided to one network, and in actual communication, a physical address (MAC address) is obtained from an IP address according to an address resolution protocol (ARP), and a communication destination is specified by the physical address so that 25 communication is held (data link layer). Normally, the physical address that is returned from the communication destination is used, but a different node can return it. This is called as the substitute ARP.

[0043] Each network is provided with an encryption server having a network router function and a substitute response function for receiving a packet instead of a receiving node. A transmitting node of the network on a transmitting side sends only data whose communication secret is desired to be kept to the encryption server, and encryption server converts the data into the encrypted data so as to transmit the data to a network of a receiving destination of this data using the network router function.

5 [0044] On the other hand, the encryption server of the network on the receiving side receives the packet (encrypted data) transmitted from the network on the transmitting side using the substitute response function for receiving the packet instead of the receiving node, and restores the packet so as to transmit the restored data to the receiving node.

10 [0045] Fig. 3 is a flow chart illustrating a flow of data when the encrypted communication is held between the node A of the IP network NET-1 to the node C of the IP network NET-3. The case where an encryption key (key code) of the encryption servers S1 and S2 is fixed is described.

15 [0046] The node A registers an address of the encryption server S1 of the local area network at the time of initialization, and the encryption server S1 is used as a default router for carrying out substitute transmission/reception.

20 Further, the node C registers an address of the encryption server S2 of the local area network at the time of initialization, and the encryption server S2 is used as a default router for carrying out substitute transmission/reception.

25 [0047] Therefore, the encryption server S1 intercepts the data to be transmitted to the node A as the substitute ARP of the node A, and similarly the encryption server S2 functions as the node for implementing the substitute ARP of the node C to intercept the data to be transmitted to the node C.

[0048] At the time of the data transmission from the node A to the node C, the node A transmits raw data to the encryption server S1. The encryption server S1 encrypts the raw data and sets the "encrypted flag" so as to transmit the encrypted data to the router R1. The encrypted data is transmitted to the routers R1, R2, R3 and R4 in this order, and then to the encryption server S2 substitute for the node C.

[0049] The encryption server S2 receives and decrypts the encrypted data, and finally transmits it to the node C. The node C receives the encrypted data transmitted by the node A from the encryption server S2 as the restored data.

10 [0050] As to the routing function of the encryption server S1 according to the second embodiment, it is only necessary to transmit all received packets to the router R1. As to the routing function of the encryption server S2, it is only necessary to transmit all received packets to the router R2.

15 [0051] In such a manner, in the case of the packet communication between a plurality of networks, namely, in the case where data is sent to a receiving destination node of an external network, when the node on the transmitting side specifies the receiving destination node and transmits data whose communication secret is desired to be kept to the encryption server, the encryption server directly communicates with the network of the receiving destination node.

20 [0052] Therefore, the node on the transmitting side does neither request the encryption server to encrypt data nor transmit the encrypted data to the receiving destination node, so that the exchange of the data with the encryption server can be simplified. That is to say, the time and traffic for 25 one reciprocation required for exchanging the data between the node and the encryption server can be saved, and the processing load on the node on the transmitting side can be reduced, thereby securing the high-speed

performance and efficiency of the data communication.

[0053] The node on the receiving side can receive the encrypted data transmitted from the node on the transmitting side by the encryption server connected to a self network as the restored data. For this reason, the time and traffic for one reciprocation required for exchanging the data between the node and the encryption server can be saved similarly, and the processing load put on the node on the receiving side can be saved, thereby securing the high-speed performance and efficiency of the data communication.

[0054]

10 [Effect of the Invention] As described above, in the local area network according to the present invention, the encryption and decoding of data are performed not by each terminal device of the network but by the encryption server in a centralized manner. For this reason, the processing load put on each terminal device can be reduced, and it is only necessary to change the 15 settings of the encryption server at the time of changing the encryption key and the encryption method in the network. As a result, a complicated operation for changing the settings of each terminal device does not have to be performed, and thus the network can be easily managed.

20 [0055] When the communication can be held between the terminal devices in a plurality of networks via an external network, even if data is transmitted/received through any network routes, the data contents are not in danger of being intercepted by outsiders on such routes.

25 [0056] Further, each terminal device in the networks transmits an encryption key necessary for the encryption or decryption of data to the encryption server, and the encryption server encrypts or decrypts the data based on the encryption key received from each terminal device, so that various encryption methods can be easily utilized.

[Brief Description of the Drawings]

[Fig. 1] Fig. 1 is a diagram illustrating a system structure of a local area network (LAN) according to one embodiment of the present invention.

[Fig. 2] Fig. 2 is a flowchart illustrating a flow of data when encrypted

5 communication is held from a node A to a node C in Fig. 1.

[Fig. 3] Fig. 3 is a flowchart illustrating a flow of data when the encrypted communication is held from the node A to node C by using a routing function of encryption servers S1 and S2 in Fig. 1.

[Fig. 4] Fig. 4 is a diagram illustrating a format of an IP header of a packet

10 transmitted/received between the nodes.

[Fig. 5] Fig. 5 is a diagram illustrating a format of an “Options” field of the IP header.

[Explanations of Letters or Numerals]

A to C: terminal device (node)

15 S1, S2: encryption server

R1 to R4: Router

NET-1 to NET-3: IP network

NET-4, NET-5: network

20 FIG. 1

1: ENCRYPTION SERVER

2: NODE

3: ROUTER

FIG. 5

25 1: OPTION TYPE

2: OPTION LENGTH

3: OPTION DATA

FIG. 2

- 1: NODE A
- 2: ENCRYPTION SERVER S1
- 3: NODE C
- 5 4: INITIALIZE
- 5: REGISTER ADDRESS OF ENCRYPTION SERVER S2 OF LOCAL NETWORK
- 6: ENCRYPTION SERVER S2
- 7: INITIALIZE
- 10 8: REGISTER ADDRESS OF ENCRYPTION SERVER S1 OF LOCAL NETWORK
- 9: TRANSMIT ONE PACKET
- 10: SET ENCRYPTION REQUEST FLAG FOR PACKET HEADER
- 11: TRANSMIT TO ENCRYPTION SERVER S1
- 15 12: RECEIVE
- 13: ENCRYPT
- 14: SET ENCRYPTED FLAG
- 15: TRANSMIT TO NODE A
- 16: TRANSMIT TO NODE C
- 20 17: WHILE PASSING THROUGH EXTERNAL NETWORK, DATA IS BEING ENCRYPTED.
- 18: TRANSMIT TO ENCRYPTION SERVER S2
- 19: SET DECRYPTION REQUEST FLAG
- 20: DECRYPT
- 25 21: SET DECRYPTED FLAG
- 22: TRANSMIT TO NODE C

FIG. 3

- 1: NODE A
- 2: ENCRYPTION SERVER S1
- 3: ENCRYPTION SERVER S2
- 4: NODE C
- 5: 5: AT THE TIME OF INITIALIZATION: USE DEFAULT ROUTER AS ENCRYPTION SERVER S1
- 6: TRANSMIT
- 7: TRANSMIT TO ENCRYPTION SERVER S1
- 8: RECEIVE
- 10 9: ENCRYPT
- 10: SUBSTITUTE RECEPTION OF NODE C
- 11: DATA IN THIS ZONE IS ENCRYPTED.
- 12: EXTERNAL NETWORK
- 13: DECRYPT
- 15 14: TRANSMIT TO NODE C
- 15: END